不正アクセスの高感度検出およびグローバル警戒機構に関する研究

伊藤 政彦†、野口 正一‡、加藤 寧+、太田 耕平*、Glenn MANSFIELD*
†株式会社NTTデータ東北支社
‡福島県立会津大学
＋東北大学情報科学研究科
＊株式会社 サイバー・ソリューションズ

1. はじめに

インターネット上の情報セキュリティ確保には、不正アクセスの発見、防止が重要だが、不正の手口は日々高度化し、従来の**個別対応では限界**がある。しかし、ネットワークの高速化に伴い膨大なアクセス情報の網羅的調査が非現実的な上、実際の検出情報は不正アクセスの「**氷山の一角**」に過ぎないことが多い。例えばセキュリティホールを探す**スキャン**の個々のアクセスは一見関連がないように見え、実時間で全体像を捉えることは容易ではない。わずかな異常から迅速に全体を検知する**高感度検出技術**が必要である。一方、不正アクセスの多くは他のサイトを踏み台として利用するため、第三者が無意識に**不正アクセスを助長**する可能性がある。不正防止には、検出のみならず、**アクセス経路の特定**が重要である。

このような背景に対応し侵入検出システム（IDS: Intrusion Detection System）の研究は広く行われているが、本研究開発は、不正防止のために重要な侵入以前の早期警戒体制への移行を可能とし、トラヒックの振る舞いをリアルタイムに捉える新手法と経路ポリシー情報に基づく診断システムを特徴とする。不正アクセスを早期に発見し、インターネット全体に渡って追跡捜査できる先進的な検出・警戒システムを開発し、情報セキュリティ分野における基盤的ソフトウェア技術の確立への寄与を図るものである。

2. 研究開発の目標と内容

本研究開発は、不正アクセスの検出と診断を行う統合システムの構築を目的とする。本システムは、膨大なトラヒック中の**微少な異常を検出**する新手法、および、**ネットワーク地図情報**と連動したアクセス経路捜査機能を特徴とする。本システムによって、高速ネットワーク上の不正アクセスの高感度検出と、その発信者、中継者、潜在的影響範囲をグローバルなインターネット規模で捜査できる不正アクセス早期警戒システムを実現することを目指す。

本研究開発は、調査研究を主体とする「研究開発」、および機能項目を実現する「研究開発のためのソフトウェア開発」（以下、ソフトウェア開発と略記）に分け実施する。

研究開発は、３つの研究開発から構成され、それぞれの研究開発項目の成果が反映される機能項目名を表 1に示す。

研究開発とソフトウェア開発の目標と内容について詳細を以下に述べる。

表 1　研究開発項目の成果が反映される機能項目名

研究開発項目	成果が反映される機能項目
実運用ネットワークトラヒックについての調査研究	リアルタイムトラヒックダイナミクス検出機能
不正アクセス検出技術についての調査研究	ネットワーク地図情報と連携した捜査診断機能
不正アクセス検出システムに必要な機能についての研究	不正アクセス早期警戒機能

2.1. 研究開発

2.1.1. 実運用ネットワークトラヒックについての調査研究

実運用ネットワークのトラヒック中に観測されるトラヒックを定量的に調査する。また、侵入検出システムの方法論を実ネットワークトラヒックの特性を基に論じ、不正アクセス検出技術の可能性を明らかにする。

2.1.2. 不正アクセス検出技術についての調査研究

不正アクセス技術について、これまでの技術と今後の動向を詳細に調査し、IDS、特にネットワーク型侵入検出システム（NIDS: Network-based Intrusion Detection System）の解決すべき技術的課題を明らかにする。

2.1.3. 不正アクセス検出システムに必要な機能についての研究

不正アクセス検出システムが備えるべきアーキテクチャとして、基本となる不正アクセス検出機能のほかに、検出システム自体の安全性、通信の機密性、完全性、および本研究開発で目指す分散システムとしての IDS に必要な機能を明らかにする。

2.2. ソフトウェア開発

2.2.1. リアルタイムトラヒックダイナミクス検出機能

本機能はユーザ要求を入力とし、パケットモニタとフィルタリングを行い、不正アクセス情報を出力とする機能を提供するものとする。パケットモニタはネットワークを流れるトラヒックを監視し、フィルタリングによって、必要なパケットを抽出する。

2.2.2. ネットワーク地図情報と連携した捜査診断機能

本機能は不正アクセス情報、ポリシー情報およびユーザ要求を入力とし、不正アクセス情報と接続ポリシー情報を連動させた捜査診断を行い、地図ベースセキュリティポリシー情報を出力とする機能を提供するものとする。

2.2.3. 不正アクセス早期警戒機能

本機能は、地図ベースセキュリティポリシー情報、不正アクセス情報およびユーザ要求を入力とし、不正アクセスが関連するサイト、管理者情報の抽出を行い、セキュリティクラブ情報を出力とする機能を提供するものとする。セキュリティクラブ情報は IRR などから得られる経路ポリシー情報に、ユーザ要求を付加したもので構成される。

2.2.4. スタンドアローン不正アクセス検出機能

本機能はユーザ操作を入力とし、不正アクセス情報、セキュリティクラブ情報、セキュリティポリシー情報にアクセスし、スタンドアローン（単独）のシステムとして不正アクセストラヒックの検出を行い、不正アクセス検出結果を出力とする機能を提供するものとする。

3. 本年度の活動状況

3.1. 研究開発

3.1.1. 実運用ネットワークトラヒックについての調査研究

本調査研究では、不正アクセスに関係するネットワークトラヒックの特性を明らかにするために、ネットワークパケットを収集する観測システムを構築し、バックボーンネットワークとLAN の 2 つの異なる環境における実ネットワークトラヒック情報を収集した。一般的な不正アクセスとそれに利用されるトラヒックの関連を調査し、現在の NIDS の可能性と問題点を明らかにした（表 2)。

表 2　NIDS の可能性と問題点

可能性	● DoS などのネットワーク資源に対する攻撃を検知できる ● 消去できない情報（パケット情報）を基礎としている ● ネットワークトラヒックは十分な情報を含んでいる ● プラットフォームに依存しない ● サービス中のシステムに負荷をかけない
問題点	● 処理能力の点で将来の高速ネットワークへの適用が難しい ● NIDS に対する固有の回避法が存在する ● トロイの木馬等の検出に向いていない

ネットワークに対する不正アクセスは必ずトラヒックとしてネットワーク上を流れ、ホスト上のログなどと異なり、削除することができない。NIDS は、ネットワークトラヒック中の不正を示す特徴（シグネチャ）に適合するパケットを検出する。シグネチャが特定のパケットに対するフィルタとして一意に記述できることからプラットフォームに依存しないシステムとなる。また、トラヒックに対して集中的に処理を行うため、エンドノードに負荷をかけない。しかし、NIDS 固有の問題点としては、NIDS を回避する不正な技術が存在すること、および性能面での拡張性が挙げられる。現実問題として、膨大なネットワークトラヒックから、100%の信頼性で特定の不正アクセスを抽出することは容易ではない。また、トロイの木馬などを検出することには向いていない。NIDS のポテンシャルを生かし弱点を補うためには、なんらかの効率的な応用が必要である。

3.1.2. 不正アクセス検出技術についての調査研究

本調査研究では、不正アクセス検出技術についての様々な活動、情報源、研究期間を調査し、不正アクセスの一般的パターンと原因について分析した。また、不正アクセス対策として今後解決していかなければならない次のような技術的課題を明らかにした。

- **ネットワークの高速化への対応：**膨大になる一方の通信内容をすべてチェックすることは現実的ではなく、全てのパケットの内容を検査する現在の方式では限界がある。

- **広域化への対応：**分散型攻撃などの不正アクセスの広域化に対して、IDS などの検出技術は各サイトに閉じた局所的なものであるため、対応に限界がある。
- **IDS 回避技術への対応：**IDS による検出を回避する技術も顕在化しており、攻撃手段がより高度かつ巧妙になっている。
- **IP address spoofing への対応：**不正アクセスの対策には攻撃者の特定が重要であるがアドレス情報を詐称する IP address spoofing によって追跡が困難である。

不正アクセス、およびその対策技術は未だ発展途上であり、上記の技術課題だけではなく今後解決すべき問題は多い。そのような中で、従来はクローズに行われていたセキュリティ技術についての議論がオープンになり、システムの弱点、セキュリティホールが公の場で議論されることが多くなっている。注目すべき点は、攻撃者達はより積極的に同様なアプローチをとっていることである。インターネット上で全世界的な協力体制を作り上げ、ソースコードを共有することで不正アクセスのための知識とツールがすばやく開発され、洗練されたものになってきている。セキュリティ対策をとる側でも同様な協調体制が必要となり、今後はよりオープンな情報共有が必要となる。

3.1.3. 不正アクセス検出システムに必要な機能についての研究

本研究では、今後の IDS に必要とされる機能について明らかにした。将来の IDS は他のシステムと協調動作することが求められ、ネットワーク管理の一要素として統合されることが期待される。次世代の IDS には次のような機能が必要となる。

- 他のシステムとの協調
- 管理システムへの統合化
- IDS 自身の安全性
- プライバシ情報の保護
- セキュリティ関連通信の機密性・完全性の確保

分散システムとしての IDS の可能性を研究し、新たな不正アクセス検出アプリケーションの開発につなげるとともに、その共通インフラである広域分散管理フレームワークの整備および標準化が必要である。分散化には分散システム間通信、IDS 自身の安全性も重要な要素となる。また、通信内容として配信される不正アクセス情報は多くのプライバシ情報を含むことが予想されることから、厳密に守られなければならない。

3.2. ソフトウェア開発

図 1に本ソフトウェア開発で開発した機能の関係を示す。ネットワークからパケットを収集し、リアルタイムトラヒックダイナミクス検出機能、ネットワーク地図情報と連携した捜査診断機能、不正アクセス早期警戒機能をスタンドアローン不正アクセス検出機能として統合する。

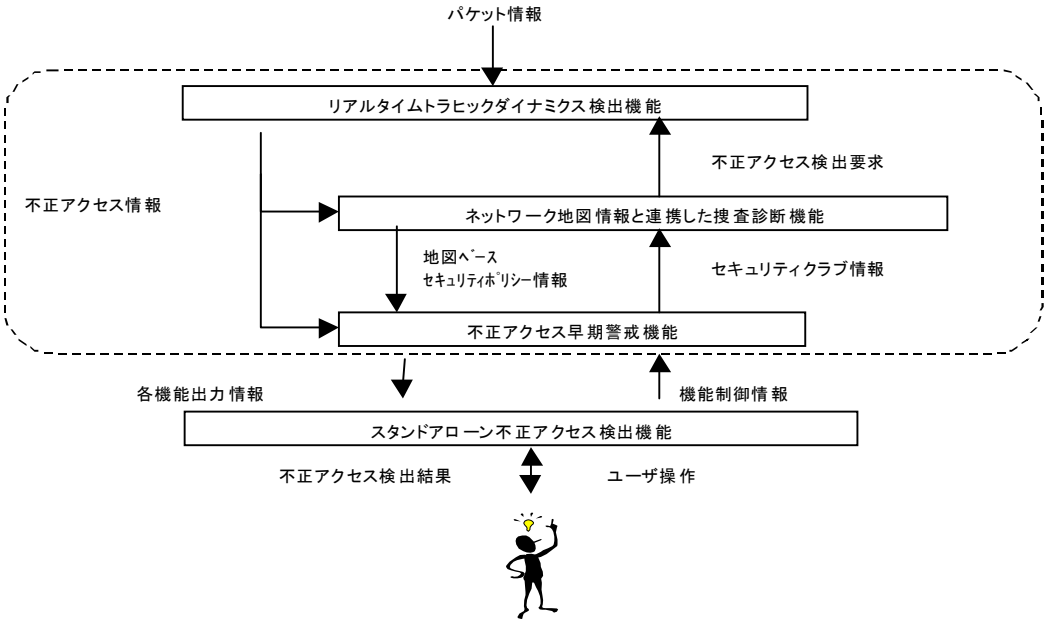

図 1 全体構成図

3.2.1. リアルタイムトラヒックダイナミクス検出機能

振る舞い DB に登録されたシグネチャに基づいて、不正なネットワークトラヒックをリアルタイムに検出するリアルタイムトラヒックダイナミクス検出機能、および GUI のプロトタイプを開発した。本機能によって任意のシグネチャを GUI によって設定することができる。本機能は NIDS の基礎部分となる動的フィルタリングを実現する。

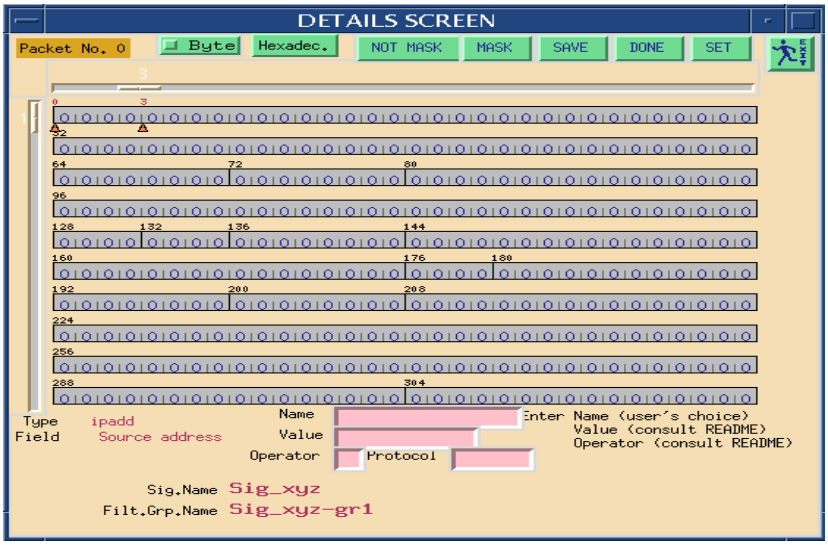

図 2 リアルタイムトラヒックダイナミクス検出機能の画面例

3.2.2. ネットワーク地図情報と連携した捜査診断機能

不正アクセス情報、ポリシー情報およびユーザ要求を入力とし、不正アクセス情報と接続ポリシー情報を連動させた捜査診断を行う捜査診断機能、および GUI のプロトタイプを開発した。平成 11 年度はローカルネットワーク上でネットワーク地図と連携する機能を研究開発した。本機能を平成 12 年度に拡張し、IRR(Internet Routing Registry)を基にしたグローバルインターネット地図上での捜査診断システムとする。

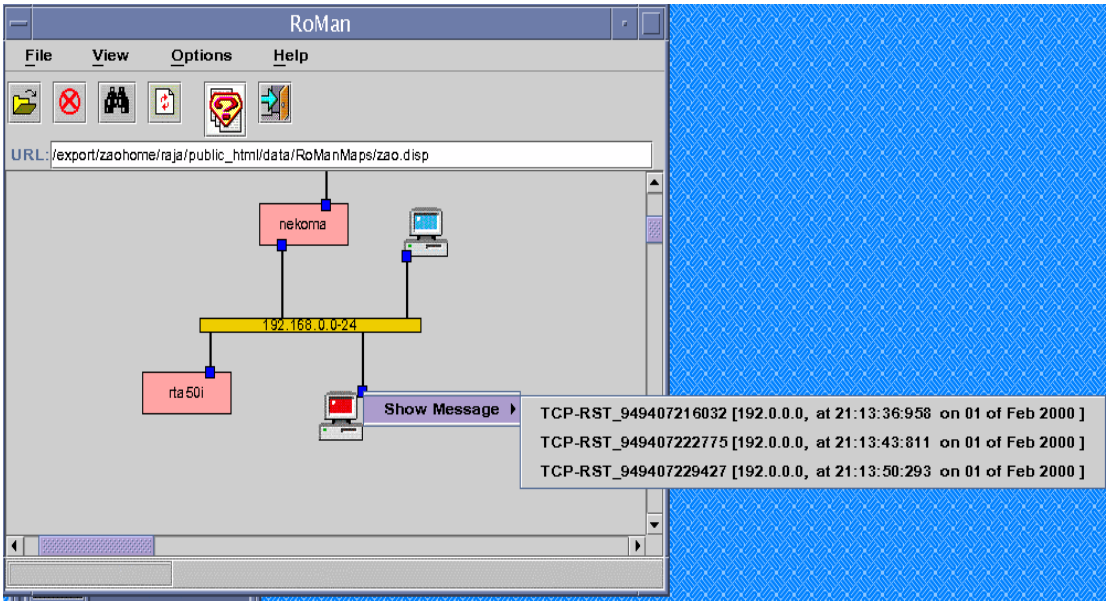

図 3　ネットワーク地図情報と連携した捜査診断機能の画面例

3.2.3. 不正アクセス早期警戒機能

不正アクセスが関連するサイト、管理者情報の抽出を行い、広域不正アクセスに関する情報を共有する早期警戒機能、および GUI のプロトタイプを開発した。振る舞い DB 管理システム、およびネットワーク地図と連携する早期警戒機能の基礎となる。平成 12 年度は、振る舞い DB の持つ情報を平成 12 年度に研究開発するセキュリティシステム間通信によって、ネットワーク上に分散配備されたスタンドアローンシステムに遠隔設定する機能を実現し、分散協調型侵入検出システムアプリケーションを研究開発する。

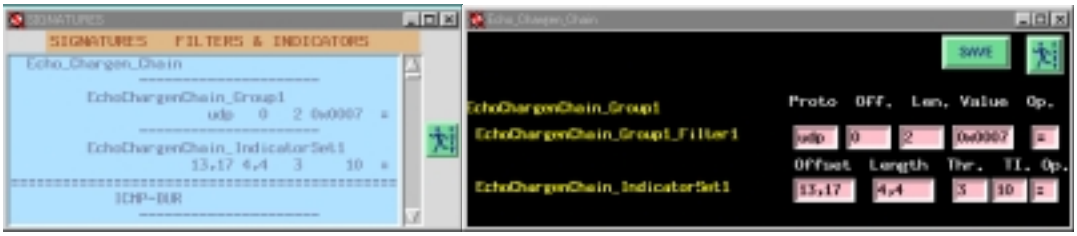

図 4　不正アクセス早期警戒機能の画面例

3.2.4. スタンドアローン不正アクセス検出機能

リアルタイムトラヒックダイナミクス検出機能、ネットワーク地図情報と連携した捜査診断機能、不正アクセス早期警戒機能を統合するプラットフォームのプロトタイプを開発した。分散システムのための通信機能などを備える基本プラットフォームとなる。平成 12 年度は、本

スタンドアローンシステムにセキュリティシステム間通信とグローバルインターネット地図をベースにしたGUIを備えるための研究開発を行い、管理システムとして統合可能にする。

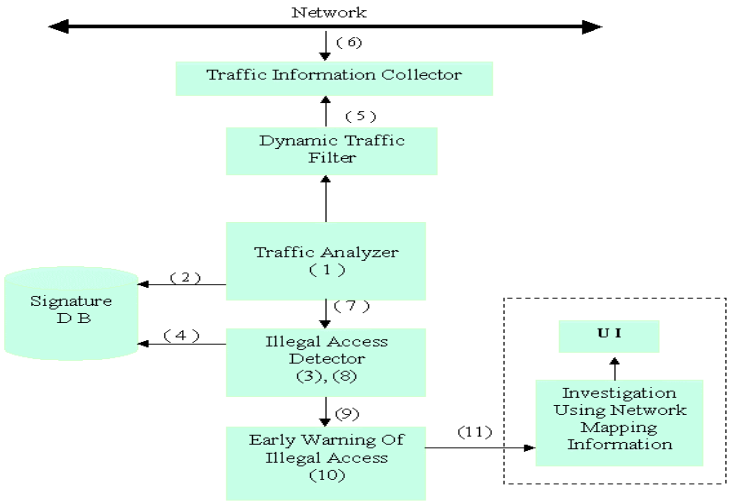

図 5　スタンドアローン不正アクセス検出機能のシステム構成

3.3. その他の研究活動

① 不正アクセス検出技術研究会：1999 年 12 月に IPA、NTT データ、東北大学、サイバー・ソリューションズ合同の不正アクセス検出技術研究会を行った。

② IDS 技術研究会：2000 年 2 月 17,25 両日に IPA で開催された IDS 技術研究会に出席し IETF における標準化活動についての発表を行った。

③ WIDE-NETMAN WG：隔週で開催しているインターネット技術についてのオープンなディスカッショングループで議論を行った。

④ IETF：インターネット技術の標準化について議論する国際的な集まりであり、IDS 通信の標準化について提案活動を行った。

4. 外部発表および成果物

4.1. 外部発表

4.1.1. 学会論文誌

① Nei Kato, Hiroaki Nitou, Kohei Ohta, Glenn Mansfield, and Yoshiaki Nemoto, "*A Real-Time Intrusion Detection System(IDS) for Large Scale Networks and Its Evaluations*", IEICE Trans. on Communication, Vol.E82-B, No.11, pp.1817-1825(1999)

4.1.2. 国際会議

① G.Mansfield, K.Ohta, Y.Takei, N.Kato, and Y.Nemoto, "*Towards trapping wily intruders in the large*", The proceedings of Second International Work-shop on Recent Advances in Intrusion Detection, West Lafayette, Indiana, USA, September 7-9,1999.

② Kohei Ohta, Yohsuke Takei, Nei Kato, Glenn Mansfield, and Yoshiaki Nemoto,

"*Synchronizing Management Information Using Traffic Pattern Matching Technique*", The Proc. of 1999 Symposium on Performance Evaluation of Computer and Telecommunication Systems, pp.349-354 (1999).

③ Glenn Mansfield et.al, "*Network Maps: Synthesis and Applications*", Proceedings of 1999 Asia Pacific Symposium on Information and Telecommunication Technologies, August, 1999

4.1.3. 国際標準化活動（IETF）

① Glenn Mansfield, Dipankar Gupta, "*Intrusion Detection Message MIB*", work in progress, http://www.ietf.org/internet-drafts/draft-glenn-id-notification-mib-01.txt, October 23 1999

② G. Mansfield, D. Curry, "*Intrusion Detection Message Exchange Format Comparison of SMI and XML Implementations*", work in progress, http://www.ietf.org/internet-drafts/draft-mansfield-curry-idmef-xmlsmi-00.txt

4.1.4. 学会発表

① 武井洋介, 太田耕平, 加藤寧, グレン・マンスフィールド, 根元義章, "*トラヒックパターンを用いた不正アクセス検出及び追跡方式*", 電子情報通信学会技術研究報告 IN99-75,(1999)

② 武井洋介, 太田耕平, 加藤寧, グレン・マンスフィールド, 根元義章, "*トラヒックパターンを用いた不正アクセス検出方式*", 電子情報通信学会情報・システムソサイエティ大会, B-7-46, p.86,(1999)

③ 仁藤浩明, 太田耕平, 加藤寧, グレン・マンスフィールド, 根元義章, "*ネットワーク履歴情報管理システムのセキュリティ管理への応用*", 1999 年電子情報通信学会総合大会, B-7-70, p.179, (1999)

4.2. 成果物

4.2.1. ソフトウェア

(1) リアルタイムトラヒックダイナミクス検出機能
(2) ネットワーク地図情報と連携した捜査診断機能
(3) 不正アクセス早期警戒機能
(4) スタンドアローン不正アクセス検出機能

4.2.2. ドキュメント

(1) 研究開発報告書
  ① 研究開発編
  ② ソフトウェア開発編
  ③ 取扱説明書
(2) 研究開発作業活動報告書
  ① 実施計画メモ
  ② 発注仕様書

③ 定例進捗報告会（第１回～第３回）議事録及び資料一式
④ 不正アクセス検出システム研究会（12／14）実施議事録及び資料一式
⑤ IETF、IDWG 等国際会議議事録及び資料一式

5. 今後の課題

ファイヤウォールに代表される従来の不正アクセス対策は、ネットワークを分断することで、不正なアクセスを防いでいた。しかしながら、近年の不正アクセスは広域化する傾向があり、攻撃者同士も協調する動きが盛んになっており、局所的なシステムでは対応困難になっている。また、IP spoofing が攻撃者の追跡を不可能にしている。

次世代の IDS は、より積極的に各種の管理システム、セキュリティシステムと連携し、広域・多様化する不正アクセスに対抗できる技術が必要となる。また、運用レベルでは、ISP、ネットワーク間の協調が重要な要素となる。現在は、異なる組織に属するネットワーク管理は管理者同士の連絡によって人手で行われている。今後の協調型の不正アクセス対策には、制御された安全な通信を通してセキュリティ情報を相互に交換できる標準技術が必要である。

6. まとめ

本研究開発では、インターネットの不正アクセスを高感度に検出できるグローバルな早期警戒機構に関する研究開発を行った。不正アクセスとその対策技術、機能要件に関する調査研究、および実ネットワークトラヒックの研究を行うことで、次世代の不正アクセス対策技術開発の基礎を確立した。また、分散型システムとなる本研究開発の最終目標のためにスタンドアローンシステムのプロトタイプ開発と国際標準化活動を行った。今後はこれらを分散システムとして構築する通信技術・プラットフォームの研究開発を行うとともに、不正アクセスの検出だけではなく対策技術の研究開発を行っていく予定である。

7. 参考文献

① 仁藤 浩明、太田 耕平、Glenn Mansfield、他, ″ネットワーク履歴情報管理システムのセキュリティ管理への適用″, 1999年 電子情報通信学会 総合大会

② Nei Kato, Kohei Ohta, Glenn Mansfield, et.al.: ″Construction of the Real-time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations.″, IEICE Trans. on Communication, Vol.E82-B, No.11, pp.1817-1825(1999)

③ "**インターネットオリエンテーリング可能な地図構成法に関する研究**", **第**17**回**IPA**技術発表会**, 1998**年**10**月**21**日**-22**日**, **新井 章治**, **野口 正一**, **太田 耕平**, Glenn Mansfield

④ IETF Intrusion Detection Exchange Format (idwg), http://www.ietf.org/html.charters/idwg-charter.html

⑤ Glenn Mansfield et.al, "*Network Maps: Synthesis and Applications*", Proceedings of 1999 Asia Pacific Symposium on Information and Telecommunication Technologies, August, 1999